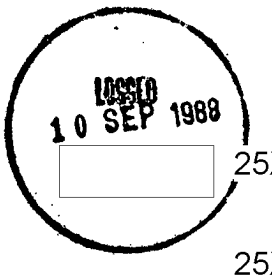
SECRET

25X1

ICS 4227-88
1 June 1988



25X1

MEMORANDUM FOR: Deputy Director of Central Intelligence

VIA: Acting Director, Intelligence Community Staff

25X1

FROM: Chairman, DCI Intelligence Information Handling Committee

SUBJECT: Multilateral Counterterrorist Data System (MCDS)

1. This is to amplify the recent memorandum to you on this subject (Reference) by Fritz Ermarth and Andre LeGallo. The IHC-proposed MCDS design and operations concept referred to therein is outlined in Attachment A hereto. Attachment B is a draft Terms of Reference for a follow-on, fast track system definition effort to examine: (a) the technical and operational implications of implementing the concept; (b) the projected cost of doing so; and (c) the willingness of the Community and other governmental agencies involved in counterterrorism to actively participate in development and support of MCDS. Favorable determinations in these areas would be logical prerequisites to any system implementation action. The proposed study would require funding for contractor technical and administrative support.

25X1

25X1

2. I am prepared to further discuss this initiative with you at your convenience.

25X1

25X1

Attachments:
As stated

cc: C/NIC
NIO/CT

25X1

SECRET

Attachment A

MCDS: Concept of Design and Operations

Principal Operational Objective

To facilitate counterterrorist operations and intelligence analysis by providing improved communications, information handling and data base access in a secure operating environment.

Basic System Design Concept

MCDS would be designed to function as a community-specific system, meaning that it would be technically and functionally structured to support a limited, pre-defined body of users, i.e., the counterterrorism community. This approach would permit adoption of technical and procedural security controls needed to maximize protection of intelligence sources and methods while facilitating a relatively uninhibited interchange of information within the community the system supports. It would also aid in tailoring system capacities and capabilities to maximize responsiveness.

MCDS would be a closed system without interactive connection to any other system. Data could be entered into the system online, but could not be transferred out of the system electronically. Outputs would be limited to system controlled peripherals (display terminals, printers, etc) that could not further transfer the data without human intervention. Additional security features would include:

- o centrally monitored terminal access control (personal identification verification)
- o automatic collection of audit trail data: user activity, internal data transfers, outputs, interstation communications, etc.
- o automated monitoring of audit data (intrusion detection expert system)
- o superencryption of data transmitted via multiuser networks, e.g. DODIIS.
- o operate as a compartmented mode system per DCID 1/16.

Operationally, MCDS would view its subscribers as members of the defined counterterrorism community rather than of a spectrum of separate agencies and commands. Dissemination of reports and access to data bases within MCDS would, therefore, be determined on a functional rather than organizational basis. An authorized MCDS subscriber would have access to all data within the system that corresponded to an established need-to-know profile reflecting the scope of his or her assigned counterterrorism operations or analysis duties.

MCDS would be established as an addressable entity for communications purposes, and would be made a direct addressee of terrorist-related message reporting and other traffic its subscriber community found operationally useful. The system would automatically route incoming traffic and provide for specific alerting. It would also accumulate daily acquisitions and make them available for retrospective search in accordance with established user profiles.

The basic system development objective would be to provide the MCDS user a fully integrated suite of facilities, data bases, and information handling services needed to support counterterrorist operations and analysis.

The underlying operational objective would be to establish channels for effective interaction among the people and organizations conducting counterterrorist analysis and operations. The episodic nature of terrorist activity and its intelligence manifestations create situations that are not readily predictable and, therefore, require ad hoc interpretations, decisions, and actions. Given the involvement of numerous, physically separated organizations with differing perspectives, knowledge bases, and operational imperatives, such situations generate discontinuities that can degrade the efficacy and timeliness of counterterrorist action. While MCDS would not of itself resolve such difficulties, it can provide a critical medium for enhancing the interaction of the people who could. Operational experience with even the limited capabilities of FLASHBOARD attests to the value of such facilities.

Next 5 Page(s) In Document Denied

Issue

The priority given by the National Security Council and by Agency management to the establishment of a computer data base for use by the counterterrorist intelligence community is not reflected in the current rate of progress toward this goal.

Background

Responding to the Congress and to NSDD 30 calling for better interagency handling of counterterrorist-related information, Director Casey committed the CIA to develop a community-wide data-base which was implemented through the creation of the Decision Support and Information System for Terrorism (DESIST) in 1984. DESIST was absorbed by the Counterterrorism Center (CTC) upon its creation in 1986. The following year, the Deputy Director for Operations (DDO) requested the Intelligence Community Staff (ICS), which concurred, to take the lead on questions related to systems interface and shared funding while CTC continued to run DESIST. ICS then began to develop a more comprehensive Intelligence Community program, not necessarily including DESIST, envisioning a possibly new community data base that would be more "user-friendly" than DESIST and promote community funding support. In November 1987, the Deputy Director of Central Intelligence (DDCI) notified National Foreign Intelligence Board principals that he had designated the ICS to coordinate the effort within the Community to ensure compatibility of systems and data structures. In December 1987, the Chairman of the Information Handling Committee (IHC) of the ICS forwarded a proposed concept of design and operations to the Office of Information Technology (OIT), CTC and to the National Intelligence Officer/Counterterrorism (NIO/CT) offering suggestions on solving the operational efficiency against security dilemma. The NIO/CT held a meeting of interested CIA representatives, which surfaced divergent views, and subsequently sent the IHC concept paper to the members of the Counterterrorism Community. Responses were supportive. Exceptions included the National Security Agency, which wanted more details before committing itself, and from Information Management Staff (IMS) of the DO which, while stating the proposal was "on track", proposed additional, and problematic security constraints (e.g. recipients of MCDS information to be polygraphed).

Problems

There is no agreement between IHC and CIA on the concept for a Community-wide database system.

There is not a designated hitter for CIA, i.e. one voice.

The role of the IHC as the coordinator and of CIA as the executive agent is unclear.

There is a chicken and egg problem; that is, whether to decide first on the system or ensure that the policies of the various players will allow their information to be included on the system.

Funds are necessary to better define the concept.